REMARKS

The application is believed to be in condition for allowance.

Claims 16-35 are pending. Claims 16 and 30 are independent.

Formal Matters

Claims 16-29 were rejected under section 112, first paragraph as failing to comply with the written enablement requirement.

The Official Action stated that the claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains to make and/or use the invention. More specifically, the Official Action stated that the "sequential" and "sequentially" limitations could not be found in the original specification.

Claims 16-29 were also rejected under section 112, second paragraph, as being indefinite. The Official Action stated that the recitation [of claim 16] "C) executing another action chain including sequentially" is not clear.

Applicant respectfully disagrees as to each of these rejections.

An abbreviated form of claim 16, prior to the present amendment, follows:

16. A data sale immediate settling method comprising the sequential steps of:

A) providing …;

B) executing a first action chain … including sequentially

i) the user inputting …,

ii) a first validation …,

iii) the user entering …, and

iv) requesting …; and

C) executing another action chain … including sequentially

i) the user inputting …,

ii) validation …,

iii) the user entering …, and

iv) requesting …,

wherein step C) is repeated.

The Claims Are Not Indefinite

First, applicant will address the section 112, second paragraph indefiniteness rejection.

The only stated basis for rejecting claims 16-29 as being indefinite was stated as the claim 16 recitation of "C) executing another action chain including sequentially" is not clear.

Applicant does not really understand what is unclear with this recitation, but in view of the section 112, first paragraph rejection, believes the use of "sequentially" is the problem.

Consider the form of claim 16 which recites three sequential steps A), B), and C). For each of steps B) and C) there is recited sequential sub-steps i), ii), iii), and iv).

See that step B) recites "executing a first action chain" and that step C) recites "executing another action chain".

In view of step B) reciting a first action chain, the recitation of another action chain is definite.

Each of steps B) and C) have the same general form, i.e., recite executing [] action chain … including sequentially i) the user inputting …, ii) validation …, iii) the user entering …, and iv) requesting …. This form is definite in that there is recited sequential sub-steps i), ii), iii), and iv). In view of the formatting of the claim, there is no doubt as to what is required.

Although not believed to be necessary, steps B) and C) have been amended to recite "executing [] action chain ~~including sequentially~~ comprising the sequential sub-steps of".

This amendment is non-substantive and introduces no new matter.

Entry of this amendment and withdrawal of the indefiniteness rejection is solicited.

If entry of this amendment is denied, withdrawal of the indefiniteness rejection is still solicited.

The Claims Are Enabled

The Official Action stated that the "sequential" and "sequentially" limitations caused the claims to contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains to make and/or use the invention. More specifically, the Official Action stated that the "sequential" and "sequentially" limitation could not be found in the original specification.

It is true that the words "sequential" and "sequentially" are not in the specification. However, that does not mean that the specification does not support these recitations. The issue is not whether these words are in the specification, but rather the issue is whether the claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains to make and/or use the invention. Since the claims do not contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains to make and/or use the invention, section 112, first paragraph is satisfied and the rejection should be withdrawn.

One of skill would be familiar with the mathematical concept of a sequence of actions, i.e., a 1st action, a 2nd action, a 3rd action, …, an n-th action, and an (n+1)-th action.

One of skill would also understand that such actions are sequential, i.e., that the actions take place sequentially. Therefore, it is clear that the specification can describe a method that includes sequential steps (steps executed sequentially) without using the words "sequential" and "sequentially".

Initially, please refer to specification page 2, beginning at line 7, wherein it is disclosed that the invention provides a data sale immediate settling method that includes actions on a purchaser's end of inputting the purchaser's ID, the n-th action of inputting the n-th password used at the n-th time to a terminal, an action of inputting the (n+1)-th password used at the (n+1)-th time to the terminal, and an action of inputting contents to the terminal. Actions on a seller's end include an action of distributing the contents to the purchaser, and an action of subtracting a price corresponding to the contents from the balance in a database. Beginning at line 17, it is explicitly disclosed that the password is changeable and that the password can be changed every time a purchase is implemented so that a security is significantly raised.

Beginning at line 24, it is disclosed that actions on the purchaser's end further include an action of re-inputting the

(n+1)-th password used at the (n+1)-th time, and the action on the seller's end is to collate an agreement between the (n+1)-th password and the re-inputted (n+1)-th password. Then, the changed passwords are commonly confirmed on the purchaser's end and the seller's end. The action on the seller's end is to register the (n+1)-th password on the basis of the collation of the agreement.

From this disclosure, one of skill would understand that the invention includes a sequence of actions, i.e., a 1st action, a 2nd action, a 3rd action, …, an n-th action, and an (n+1)-th action. Further, one of skill would also understand that these actions are sequential, i.e., that the actions take place sequentially. Therefore, even though the words "sequential" and "sequentially" are not used, the specification discloses the inventive method as including sequential steps (steps executed sequentially).

Reference is next made to the DESCRIPTION OF THE PREFERRED EMBODIMENT section of the specification, as well as the drawing figures.

Claim 16 recites a first step of "A) providing a user with a prepaid card linked to a database;".

See page 6, beginning with line 5 disclosing that in an embodiment with the real (physical) prepaid card, a serial number, a first-time password number, and an expiration date are visibly printed. As shown in Figure 1, there are registered to

the database a serial number (100001), a first-time password number (36736492), a user set password number (blank), a card face value (3000), the balance (3000), etc. that all have a one-to-one correspondence with those of the specified prepaid card.

One of skill would understand that the user must be provided with the prepaid card linked to the database before, either steps B) and C) can be performed. See that step B) requires inputting a password number and comparing the input password number to the first-time password number. Therefore, it is clear that the recitation of step A) preceding steps B) and C) is subject matter which described in the specification in such a way as to enable one skilled in the art to which it pertains to make and/or use the invention, and that section 112, first paragraph is satisfied.

Figures 2-3 (beginning at line 26, specification page 6) illustrate the invention's method steps, in particular steps B) and C).

Actions 1-4 disclose inputting the card's serial number and confirming that the card is usable.

Actions 5-8 relate to the user input the initial password number (step B), sub-step i) and confirmation of whether or not the user-input password number has a one-to-one correspondence with the serial number to the database in order to allow the user further access(step B), sub-step ii).

That steps i) - ii) must necessarily follow in sequence is clear from this disclosure.

Action 9 discloses the portal site requesting the user to input the password number to be used at the next time. Actions 10-16 are the user inputting and confirming the next-time password number used for the access at the next time, and the next-time password being stored in the database (step B), sub-step iii).

Actions 16-32 relate to the user's transaction and updating the balance on the card (step B), sub-step iv).

From this disclosure, it is clear that the specification discloses that steps i) - ii) precede steps iii) - iv), and that step iii) precedes step iv).

Therefore, from the above there is disclosure of step A) preceding Step B) and steps i) - iv) being executed sequentially. In view of this disclosure, this subject matter is described in the specification in such a way as to enable one skilled in the art to which it pertains to make and/or use the invention, and section 112, first paragraph is therefore satisfied.

Figure 3, actions 33-34 disclose ending the transaction and closing the link to the database. Action 35 is the portal site returning to the input waiting for the serial number of the card (as per step C and the wherein clause).

Returning to claim 16, the above passages and figures disclose 1) providing a user with a prepaid card linked to a database; and 2) executing an action chain including validating the prepaid card by comparing a user-input password number, input by the user, with a current password number stored in the database. There is also disclosed that 1) a first validation of the prepaid card uses a system-set first-time password number stored on the database as the current password number, 2) after each validation, the user sets a new user-set password number as the current password number stored in the database.

As summarized on specification page 11, beginning with line 6, in this manner, the password number is changed every time of use so that the higher security is sustained (as per step C and the wherein clause). It is unnecessary to certify information related to an individual such as a credit card number, bank account number, address, or name when the card is used. Therefore, the card can be a gift or be used for a promotion of a company. By recording a kind, date, and volume of the transacted contents on the database of the password number and the serial number of the card, information used for market research can be collected.

Therefore, from the above it can be seen that there is disclosure of step A) preceding Step B) and steps i) - iv) being executed sequentially, as well as Step B) preceding Step C), wherein Step C) is repeated. In view of this disclosure, the

subject matter of claim 16 is described in the specification in such a way as to enable one skilled in the art to which it pertains to make and/or use the invention, and section 112, first paragraph is therefore satisfied.

Withdrawal of the Section 112, first paragraph is therefore solicited.

There are no further formal matters pending.

Substantive Matters

The following rejections are based on the text of Official Action, pages 3-13.

Claims 16-21 and 30-33 were rejected as obvious over KWAN 2003/0200179 in view of PARRILLO 5,239,583.

Claims 22-26 and 29 were rejected as obvious over KWAN in view of PARRILLO, and further in view of RUBIN 6,701,522.

Claims 27-28 were rejected as obvious over KWAN in view of PARRILLO and RUBIN, and further in view of NOVOA 6,636,973.

Claims 34-35 were rejected as obvious over KWAN in view of PARRILLO, RUBIN, and NOVOA.

Applicant respectfully disagrees.

Although user inputting new passwords is known, the applied art teaches to automate the changing of passwords, thereby avoiding requiring the user inputting new passwords each time an account/card is accessed.

KWAN does not teach the present invention's concept of having a user-supplied password set as part of each card validation and prior to accessing the card's monetary balance.

This approach provides both a convenient and elegant solution not taught or suggested by the applied art.

KWAN takes an opposite approach to that of the invention; that is, KWAN uses the system to set each next password number, e.g., codes are set by the merchant and the customer must accept the merchant-set code and later re-input the merchant-set code in order to validate the prepaid card.

As to recited step B), the Official Action (page 5, lines 1-2) acknowledges that KWAN does not disclose sub-step iii) the user entering a next-time password number and storing the user-input next-time password number in the database as a new, user-set next-time password number.

As to recited step B), the Official Action implicitly acknowledges that KWAN cannot disclose sub-step iii) being performed after sub-step ii) and before sub-step iv).

As to recited step C), the Official Action (page 5, lines 1-2) acknowledges that KWAN does not disclose sub-step ii) validation of the prepaid card by a successful comparison of the user-input another password number to the stored new, user-set next-time password number, and sub-step iii) the user entering another next-time password number and storing the user-input another next-time password in the database as the new, user-set

next-time password number required for validation of the prepaid card in a next another action chain.

As to recited step C), the Official Action implicitly acknowledges that KWAN cannot disclose sub-step iii) being performed after sub-step ii) and before sub-step iv).

On pages 5-6 of the Official Action, there is a paragraph that lists "well known" actions to improve computer account security. However, none of these actions is the missing subject matter of the independent claims. Additionally, it does not appear that any of the "well known" actions listed on pages 5-6 are prior art to the present invention.

In judging whether certain claimed features of an invention were obvious, one must be careful to place oneself in the shoes of one skilled in the art at the time of the invention. The present rejection appears to be based on hindsight, taking into account what is well known as of the present. Such an approach is not permitted.

On page 6 of the Official Action, PARRILLO is offered as teaching the user entering a next-time password as a new, user-set next-time password number.

However, the PARRILLO password is not a user-set password as required by the claim.

See the PARRILLO Abstract which discloses that the user enters a PIN code in accordance with a prescribed, but variable, sequence, the sequence being different for each transaction from

the previous transaction. The user inputs the PIN by entering a sequence of alphanumeric symbols in accordance with a prescribed "start" sequence of symbols for recognition as a proper 4-digit PIN for a first transaction. Preferably, the sequence of symbols comprising the PIN has only one symbol different from the "start" sequence for recognition as a proper PIN for a second transaction and the third transaction may require yet a third sequence of alphanumeric symbols comprising a third PIN.

The Official Action has offered column 2, lines 10-46.

This passage discloses that the use of personal identification numbers (PINs), including using PINs by many banks in their automatic teller machine apparatus.

This passage, however, only discloses use of PINs and does not disclose the features missing from claim 16.

The Official Action offered column 6, lines 26-50.

This passage only teaches the conventional (pre-PARRILLO) use of PINs (see lines 50-59).

The Official Action has offered column 3, line 58 to column 4, line 25.

This passage discloses that the PARRILLO invention provides an improvement in account access security by eliminating the possibility that repeating an exact access code. This passage teaches entering the user PIN code in accordance with a prescribed, but variable, sequence, the sequence being different

for each transaction from the previous transaction. Specifically, the passage teaches that in "the broadest aspect of the invention, the user inputs the PIN by entering a sequence of alphanumeric symbols in accordance with a prescribed 'start' sequence of symbols for recognition as a proper 4-digit PIN for a first transaction". The system, upon recognizing the correct PIN will give the user access to the account.

See column 3, line 68 that expressly teaches "At the same time, the system increments at least one of the digits of the stored PIN for that account so that, in effect, the user must enter a new PIN to access the same account on subsequent tries."

See also beginning at line 12 of column 4: "To illustrate, when the user is prompted to key in his or her 4-digit unique PIN, he or she will enter the first three digits the same for each transaction. However, the fourth digit will be different for each transaction for a sequence of, for example, four transactions. … As an example, suppose the user's first three digits of the PIN are 1, 2, and 3. The variable fourth digit can be … 8, 6, 2, and 9, respectively. Therefore, upon entering the PIN for the first transaction, the user would enter 1, 2, 3, 8 where the first three digits are fixed and the fourth digit is the first digit (8) …. If, later in the day, the user wishes to make a second transaction, when prompted for his 4-digit PIN, he or she would again enter 1, 2, 3, but this time the fourth digit would be a 6, …. This process would continue until

the user has made four transactions... Of course, the system can be programmed to make any one of the four digits of the PIN variable, ..." See column 4, lines 26-57.

From these passages, it is clear that the system is in control of setting and remember the passwords. What PARRILLO teaches is that each successful login by the user causes the system to increment to the next system-set password. It is this system-set password that must be entered in the PARRILLO as part of the next transaction login.

Thus, although the PARRILLO user enters a different passage each for each transaction, it is a system-set password and not a user-set password.

Thus, the first part of step B), sub-step iii) and of step C), sub-step iii), i.e., the user entering a new, user-set next-time password number is not disclosed.

Further, claim 16 requires that the user enter this next-time password prior to sub-step iv) of requesting a current monetary balance available on the prepaid card number. In PARRILLO, the teaching is that, upon a successful login "at the same time, the system increments at least one of the digits of the stored PIN" (line 68 of column 3 and line 1 of column 4). This action does not involve the user inputting the next-time password. PARRILLO allows the transaction (including step iv) and only thereafter when the user wishes to make another

transaction is the next-time password input by the user (corresponding to step C), sub-step i).

Additionally, although PARRILLO teaches that the system increments the PIN, there is no disclosure that the system stores the new PIN (the sequence of PINs may be pre-established and incrementing moves from on PIN to an new previously stored PIN).

Further, see that step B), sub-step iii) and step C), sub-step iii) explicitly require "storing the user-input next-time password number in the database as a new, user-set next-time password number," (again prior to sub-step iv). Thus, even if a new password were stored in PARRILLO, the new password is not a user-input password as required by the claim.

Nor is there any teaching of the user-input and storing of the user-input next-time password number sub-step being performed prior to requesting a current monetary balance available on the prepaid card during a current transaction.

In this regard, PARRILLO, KWAN, and NOVOA are the same in that the user does not set the password. See in NOVOA column 3, lines 6-25 it is disclosed, beginning at line 15, (emphasis added) "At some point during or after the log on process, a biometrics account manager which has access to the users database changes the current password associated with the use to a new password. Because the user is not required to remember and type the password, the passwords may be longer and more complex, thereby further enhancing security." If the user is not required

to remember the password, it is clear that the user need not enter the new password at a later time. This passage explicitly states that the user does not type the password.

See column 3, lines 26-30 stating that the password is generated randomly. See also column 9, lines 2-9. The new password is used to log on the user; however, the user does not enter the new password. The user does not select or enter the next-time password into the system during the current password validation.

Thus, each of these references teaches completely opposite to the recited invention where, the invention provides that the user inputs a new next-time password after entering and verifying the current password.

Recall, the obviousness test is not whether the prior art included the necessary knowledge to make it possible to modify KWAN to achieve the presently claimed invention, but rather the test is whether there is motivation to modify KWAN to achieve the presently claimed invention.

The present rejection arises from improperly application of hindsight.

For a prepaid card linked to a database, the applied art does not teach or suggest executing a first action chain for immediately settling a data sale which includes sequentially i) the user inputting a password number, ii) a first validation of the prepaid card by comparing the user-input password number to a

system-set first-time password number stored on the database as the current password number, and iii) the user entering a next-time password number and storing the user-input next-time password number in the database as a new, user-set next-time password number, and iv) requesting a current monetary balance available on the prepaid card.

Nor do the references teach repeatedly executing further action chains including sequentially i) the user inputting another password number, ii) validation of the prepaid card by a successful comparison of the user-input another password number to the stored new, user-set next-time password number, iii) the user entering another next-time password number and storing the user-input another next-time password in the database as the new, user-set next-time password number required for validation of the prepaid card in a next another action chain, and then iv) requesting another current monetary balance available on the prepaid card.

The Federal Circuit has held that in determining the differences between the prior art and the claims, the question under 35 USC 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983).

Any motivation to modify KWAN to satisfy the present claims is merely hindsight with the present disclosure being used

to render the claimed invention obvious. Such an approach is not permitted.

The Federal Circuit emphasized in July, 1998 that "[m]ost, if not all, inventions are combinations and mostly of old elements." *In re Rouffett*, 47 USPQ 2d 1453, 1457 citing to *Richdel, Inc. v. Sunspool Corp.*, 219 USPQ 8, 12 (Fed. Cir. 1983). The Federal Circuit continued by noting that "rejecting patents solely by finding prior art corollaries for the claimed elements would permit an examiner to use the claimed invention itself as a blue print for piecing together elements in the prior art to defeat the patentability of the claimed invention."

Thus, the Federal Circuit requires that in order to prevent the use of such hindsight, the Official Action must "show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed." (*In re Rouffett* at 1458). The present rejection fails to meet this requirement.

The obviousness rejection is not viable.

The Official Action lastly offered PARRILLO claim 1.

Claim 1 is reproduced (in abbreviated form below).

1. A method of controlling access to a credit account ... comprising the steps of:

(a) initiating a first transaction...;

(b) selecting a first stored access code responsive to entry of, and corresponding to, said account information data block;

(c) receiving a first user entered access code;

(d) comparing said selected first stored access code with said user entered access code, and, upon a match therebetween, enabling access to said credit account for successfully conducting and concluding said first transaction;

(e) disabling access to said credit account after said first transaction is concluded;

(f) replacing said first access code stored in said storage means wit (sic) a second access code different from said first access code;

Note that, contrary to the presently claimed invention, PARRILLO claim 1 recites completing the transactions (i.e., sub-step iv) prior to replacing the first access code with a second access code. Thus, although PARRILLO does not teach sub-step iii) as recited, PARRILLO teaches that sub-step iv) is performed before the password change recited in the claim's substep iii).

From the above, it is clear that PARRILLO does not teach the recited features of the independent claims that are missing from KWAN. Therefore, the combination of KWAN and PARRILLO does not render obvious these claims.

As to claims 20 and 32, KWAN is not seen to have the recited database structure. Please identify where KWAN discloses both a field for the original password and another field for a user-set next-time password. In view of this shortcoming, this claim cannot be said to be rendered obvious.

As to claim 30, the proposed combination of KWAN and PARRILLO do not teach the claimed step of "as part of each validation and prior to accessing a monetary balance of the user's card, the user sets a new user-set next-time password as the current next-time password stored in the database".

Thus, claim 30 is non-obvious.

Claim 27 recites that after validation of the prepaid card, the portal site i) requests the user to input the new user-set next-time password number, ii) receives the new user-set password number from the user, iii) sends the received new user-set next-time password number to the database to be stored, in the user-set next-time password number field, as the next-time password number required for a next validation of the prepaid card.

NOVOA has been offered for this recitation. The Official Action refers to NOVOA Abstract, column 2, lines 27-49; and column 3, lines 6-25.

Applicant respectfully disagrees.

NOVOA does not teach that, after each of plural password validations, the user sets a new password number as the

current password number stored in the database, Rather, column 2, lines 35-39 refers to prior art to NOVOA and not to the NOVOA system. In NOVOA, the password may be changed, but not by the user.

At some point during or after the log on process, the biometrics account manager changes the current password associated with the user to a new password and overwrites the previous password with the new password.

There is no disclosure in the Abstract of the concept of the user resetting the password after each existing password validation.

Indeed, see in column 3, lines 6-25 it is disclosed by NOVOA that beginning at line 15 (emphasis added) "At some point during or after the log on process, a biometrics account manager which has access to the users database changes the current password associated with the use to a new password. Because the user is not required to remember and type the password, the passwords may be longer and more complex, thereby further enhancing security." If the user is not required to remember the password, it is clear that the user need not enter the new password at a later time. This passage explicitly states that the user does not type the password.

See column 3, lines 26-30 stating that the password is generated randomly. See also column 9, lines 2-9. The new password is used to log on the user; however, the user does not

enter the new password. The user does not select or enter the next-time password into the system during the current password validation.

Claim 35 is similar and is non-obvious for the same reasons.

Withdrawal of these rejections is solicited. If the rejection is not withdrawn, it is requested that the individual parts of the claims be identified with corresponding passages of NOVOA.

From the above it is believed to be clear that the claims are non-obvious. Reconsideration and allowance of all the claims are respectfully requested.

Applicant believes that the present application is in condition for allowance and an early indication of the same is respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

Roland E. Long, Jr., Reg. No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

REL/mjr